

Adli Rapor - Ön çalışma

Joshua Marpet

Guarded Risk, Veri Güvenliği ve Adli Danışmanlık, Yönetici Müdür

28 Şubat 2014

Genel Bilgiler:

Bu rapor, Guarded Risk yöneticisi Joshua Marpet tarafından yazılmıştır. Joshua Marpet, Wilmington Üniversitesi, Teknoloji Fakültesi, Bilgisayar Ağ Güvenliği bölümünde, Dijital Adli İncelemeler, Veri Güvenliği, Etik ve Etik Bilgisayar Korsanlığı (Hacking) eğitimi veren bir misafir öğretim görevlisidir. Joshua, dijital adli incelemeler alanında, AccessData sertifikasına (Accessdata Certified Examiner - ACE) sahip bir müfettiştir. Geçmişte, Philadelphia Merkez Bankası'nda Veri Güvenliği Kıdemi Analisti olarak görev almıştır. Veri güvenliği üzerine yürütülen Information Security Conferences (Veri Güvenliği Konferansları) Security BSides Delaware serisinin eş-organizatörlüğünü yapmaktadır ve Bulut Bilişim Güvenliği Birliği (Cloud Security Alliance - CSA) , Delaware Valley Bölge (CSA-DV) başkan yardımcısıdır. Özgeçmişinde, Katrina Kasırgası öncesinde, sırasında ve sonrasında St. Tammany Parish Sheriff's Office'te polis memurluğu vardır. Joshua Marpet'in tecrübeleri arasında, dünyanın birçok yerinde yaptığı video ve ses güvenlik sistemleri üzerine çalışmaları vardır; bunların arasında, Lower Manhattan Surveillance Initiative (Lower Manhattan Gözetim Girişimi), Cezayir Ordu Askeri Üssü Çit Alarm Sistemleri ve New Jersey'deki Newark Havalimanı Pistlerinin gözetimi, birçok cezaevi ve kumarhaneler mevcuttur.

İstenen:

Sağlanan bir MP3 dosyası üzerinde, herhangi bir "oynama" olup olmadığının, olabildiğince kesin bir biçimde belirlenmesi.

Sorunlar:

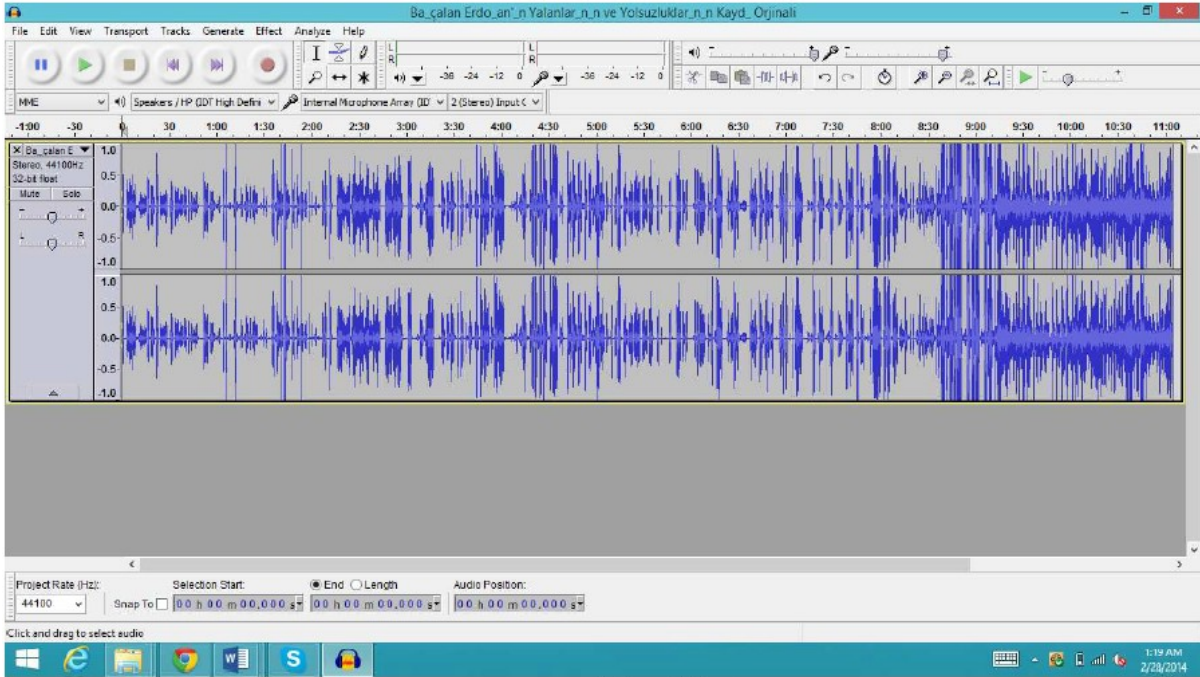
Ana dili Türkçe olmadığından; tonlama değişiklikleri, nüanslar, ton değişimleri, kelime veya kalıpların aniden kesilip kesilmedikleri ya da uyumlu olup olmadıklarını anlamak zor olmuştur. Bununla birlikte, ses dosyasının teknik bir analizinin yapılmasına ve olası anormaller ve soruların ana dili Türkçe olan kişilerin yardımıyla yanıtlanmasına karar verilmiştir.

Kullanılan Araçlar:

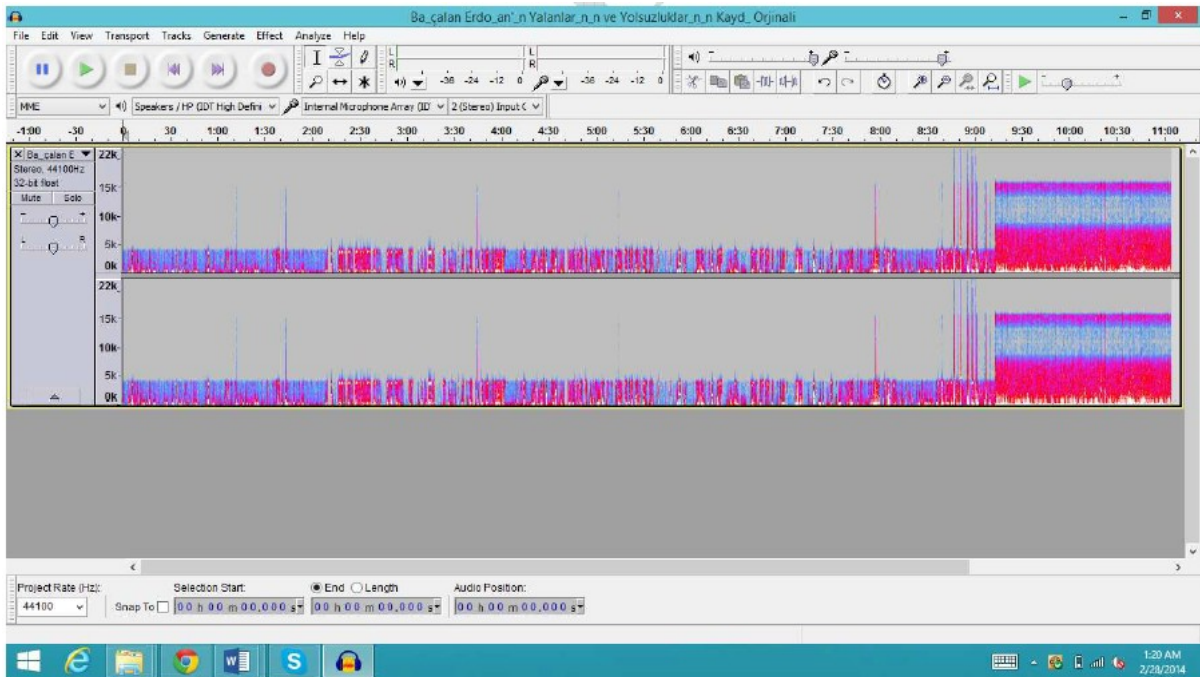
Üzerinde, tüm yamaları yapılmış, Microsoft Windows 8.1 işletim sistemi çalıştıran ve analizi gerçekleştirmek için kullanılan, HP marka bir adet dizüstü bilgisayar. Kullanılan yazılım, <http://audacity.sourceforge.net/> adresinden edinilebilen, *Audacity*. Bu yazılım, podcast (dijital medya dosyalarının -örn. Radyo yayınları-, internet üzerinden akış yoluyla dağıtılması tekniği) yaratılması ve düzenlenmesi, müzik düzenlemesinde (editing) ve karıştırılmasında (mixing) ve birçok farklı amaçta kullanılan, son derece becerikli bir yazılımdır. Açık kaynak kodlu bir yazılım olduğundan, kodları yüz binlerce kişi tarafından incelenmiş ve test edilmiştir.

Analiz:

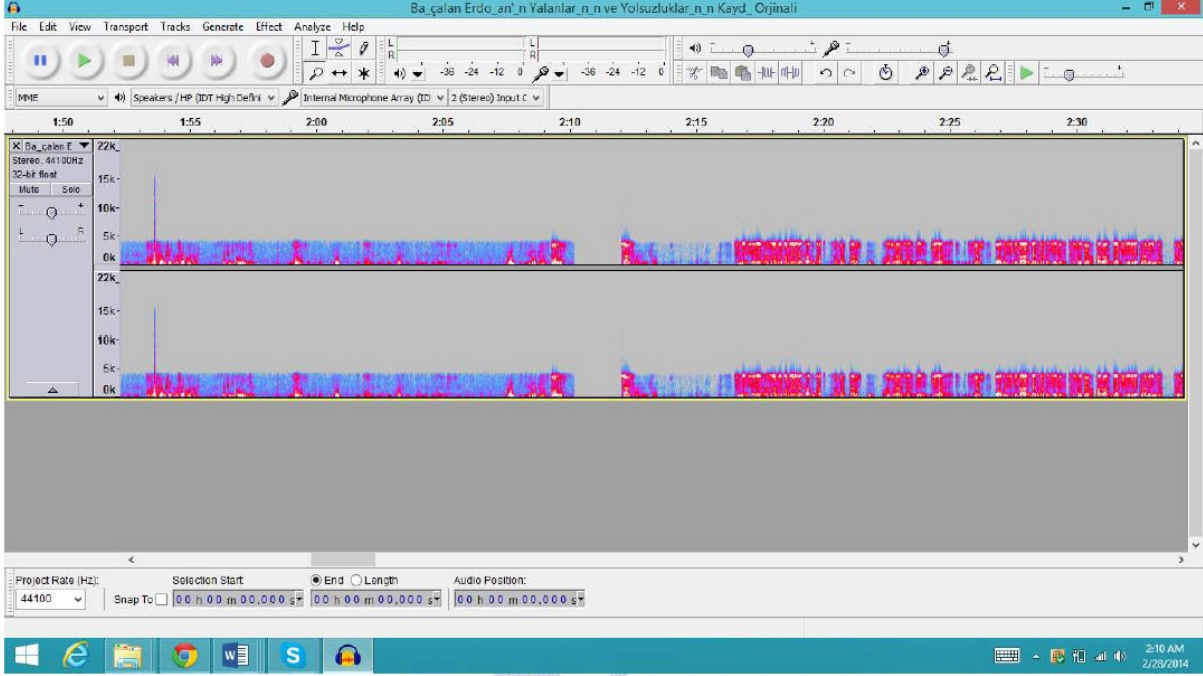
“Ba_çalan Erdo_an'_n Yalanlar_n_n ve Yolsuzluklar_n_n Kayd_Orjinali.mp3” adlı bir dosya, analiz edilmesi için ulaştırıldı. Dosya, Audacity yazılımıyla açıldığında kabaca ses seviyelerini gösteren dalga formu görülmektedir.



Spektrogram (izge grafiği) görünümüne geçildiğinde, frekans grafiği görülmektedir.



Analizde kullanılan ana görünüm olan bu görünüme geçildiğinde üç grup anormali keşfedilmiştir. Konuşmanın çoğu aynı seviyede (*noise floor* - gürültü tabanında) iken, ses dosyasının belirli yerlerinde ani frekans sıçramaları (*spike*) görülmekte, yaklaşık 9:15 itibariyle olan son birkaç dakikası ise tamamen farklı bir gürültü tabanında. Sonlardaki anormaliler, yalnızca grafiğe yaklaşıldığında (zoom yapıldığında) görülebilmekteler.



Yukarıda görülen, yaklaşık olarak 2:10 ve 2:12 aralığında, hiçbir ses içermeyen bir boşluk mevcut. Bu MP3 dosyası dinlendiğinde, kimse konuşmadığında dahi, çevresel ve elektronik sesler, örneğin, klima, ısıtma sistemleri, telefondaki hat gürültüsü, v.s. mevcut. Ancak 2:10 ile 2:12 arasında, hiçbir şey yok.

Ani frekans “sıçramaları”ndan biri, yukarıda görülen şekilde de, 1:54'ten hemen önce görülebilmekte.

Üç grup anormalinin de kötü niyetle oluşturulmuş olduğunu varsayarsak, boşluklar, ses parçalarının kesilip yapıştırılmış olduğunun; sıçramalar da bir kelimenin ya da kalıbın tonunun, tonlamasının, nüansının ya da anlamının değiştirilmiş olduğuna işaret ediyor olabilir. Son birkaç dakikadaki yükselmiş gürültü tabanı ve farklı sesler, farklı bir tür “böcek” (telefona yerleştirilen bir böcekten ziyade odaya yerleştirilen bir böcek) kullanıldığına işaret ediyor olabilir. Buna alternatif olarak, basit bir biçimde, yalnızca, aynı telefon ile, telefonun hoparlörü açılarak konuşmaya devam edilmiş olabilir.

Ana dili Türkçe olan birine danışılması sonrasında:

Anormaliler hakkında, ana dili Türkçe olan birine danışıldı.

Öncelikle, görülen, 2:10'daki gibi boşluklar tartışıldı. Öğrenildi ki, boşluklar basit bir biçimde, yalnızca, birden çok konuşmanın birleştirilip tek bir MP3 dosyasına yerleştirildiği yerlerde mevcut. Hiçbir kötü niyetle yapılmış müdahale söz konusu değil.

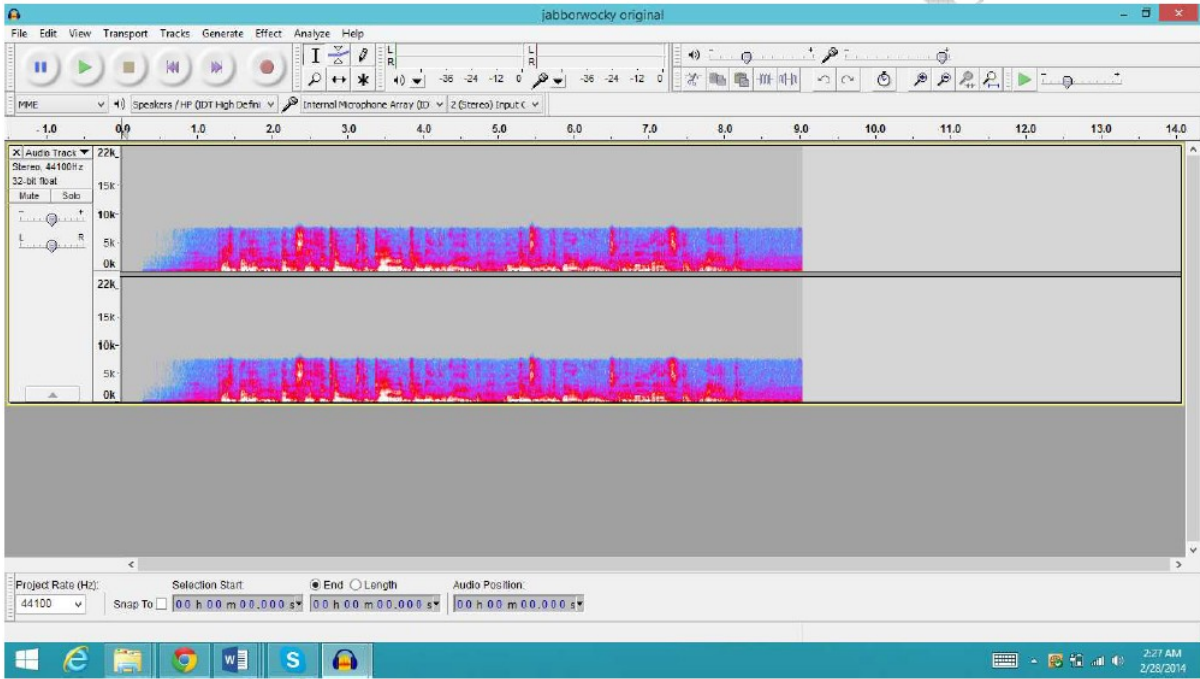
Son birkaç dakikadaki yüksek gürültü tabanının alay etme amaçlı olabileceği ya da telefon görüşmeleri ile bir ilgisi olmayan kişilerin diyalogunun eklentisi olabileceği kanısına varıldı. Telefon konuşmalarını sızdıran kişilere ait olabileceği tahmin edildi?

Çözümüne kavuşturulmamış tek anormali ise “sıçramalar” oldu. Göz önünde bulundurulmuş iki olasılık, seslerin kesilip yapıştırılmış olabileceği, bir kelime ya da kalıbın tonunun, tonlamasının, nüansının ya da anlamının değiştirilmesi çabası oldu. Ana dili Türkçe olan kişi, ton, tonlama, nüans ve anlamın tamamen doğal olduğunu ve suni bir müdahale olmadığını belirtti. Bunun yanında, sıçramaların, neredeyse her seferinde, ses hal-i hazırda başladıktan sonra ortaya çıktığı görüldü. Bu da, kesme-yapıştırma olsaydı, sesin, bu anlarda ani ve beklenmedik bir biçimde değişmiş olduğu -örneğin, bir kelimenin ortasında- görüldü demek oluyor.

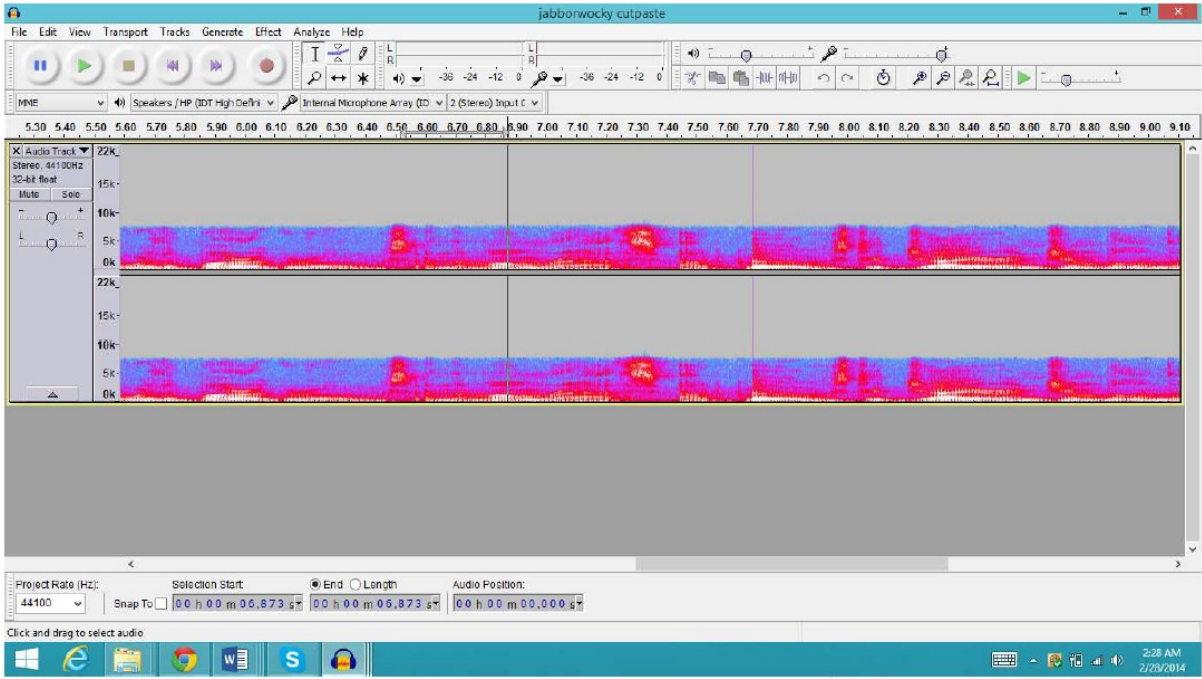
Bir varsayım, ya da tahmin, bu sıçramaların, bir tür yer işareti ya da gösterge olabileceği yönünde. Bunların çoğu, isimlerin olduğu yerlerde ya da yakınlarında gibi görünüyor. Bu durum, zamanın kısıtlı oluşundan dolayı incelenmedi.

Sonuçlar

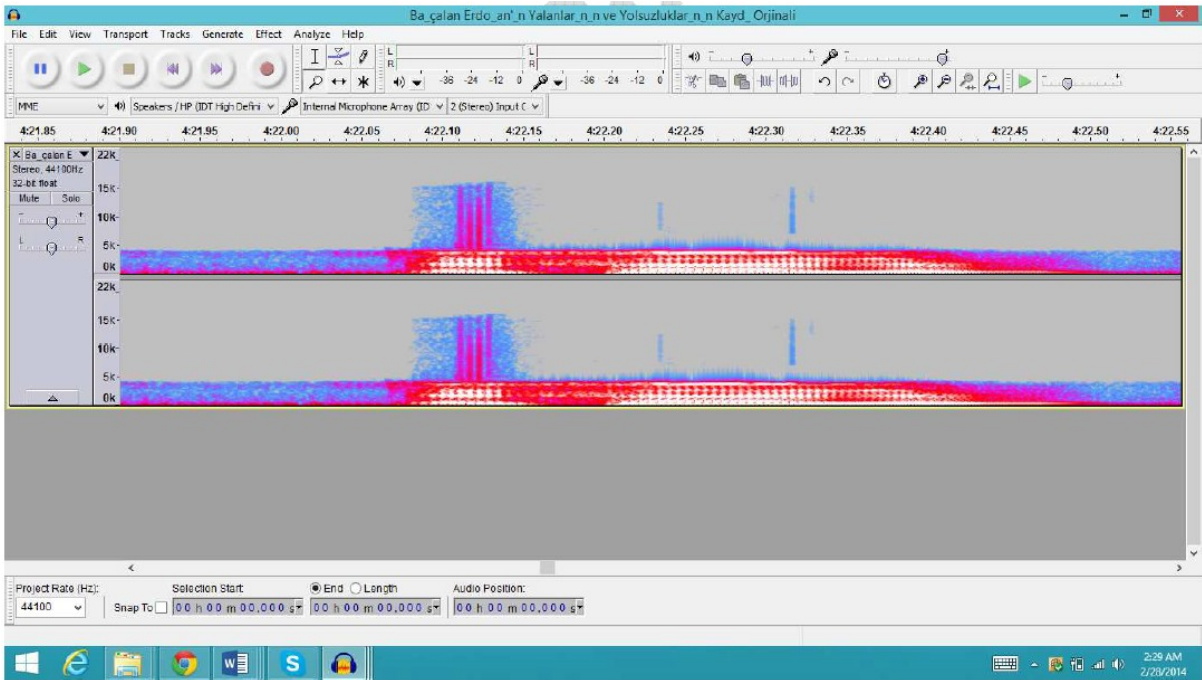
Bu kanı ve varsayımları kontrol etmek için, bu raporun başında listelenen “Kullanılan Araçlar” listesinde bahsedilmiş olan, HP marka dizüstü bilgisayar ve Audacity yazılımı kullanılarak, kısa bir ses kaydı yapıldı. Joshua Marpet, bir Lewis Carroll eseri olan, “Jabberwocky” adlı şiirin ilk dördlüğünü kaydetti.

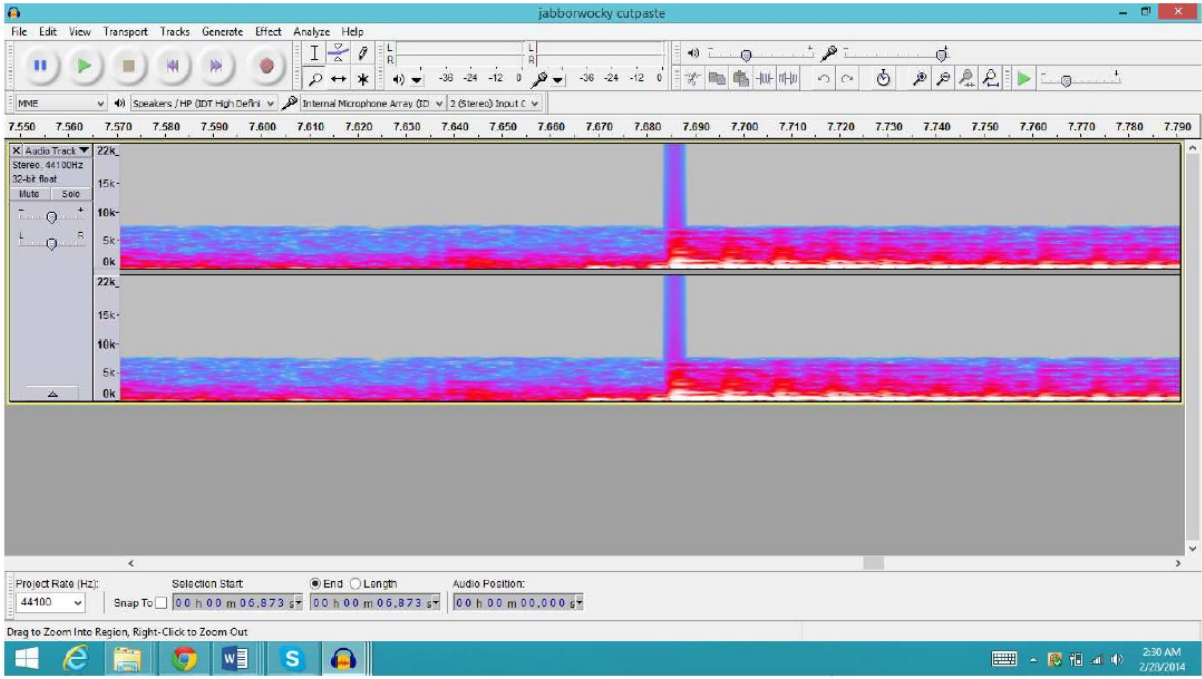


Daha sonra, bu kaydın bir kısmını kesip, şiirin daha ilerideki bir kısmına yapıştırdı.



Bazı yönlerden, incelenen ilk ses kaydındaki frekans sıçramalarına benzeyen iki sıçramaya dikkat edin. Ancak bu sıçramalar, bazı önemli açılardan, incelenen ilk kayıttakilerden farklılık gösteriyor. Grafiğe yaklaşıldığında (zoom in), bu farklar bariz bir hal alıyor.





Jabberwocky kaydında bu çizginin ne kadar net olduğuna, ve çizginin kanalın/spektogramın en yüksek noktasına nasıl ulaştığına dikkat edin. Türkçe olan arama kaydında, net de olmayan pek çok çizginin olduğuna, etraflarındaki statik seslere, ve onların kanalın/spektogramın en yüksek seviyesine ulaşmadığına dikkat edin.

Bu gösteriyor ki, ani frekans sıçramaları yapay, ancak büyük ihtimalle bir hat gürültüsünden, çıtırtıdan, ya da bizzat, pekala bir çeşit indexleme ve işaretleme sisteminden kaynaklanıyor. Türkçe bilen kişiyle kontrol edildi, bu Türkçe arama kaydında bulunan ani yükselmeler isimlerin ve kelimelerin ortasında. Herhangi bir kesme ve yapıştırma bu isimleri ve kelimeleri bozardı.

Nihai sonuçlar:

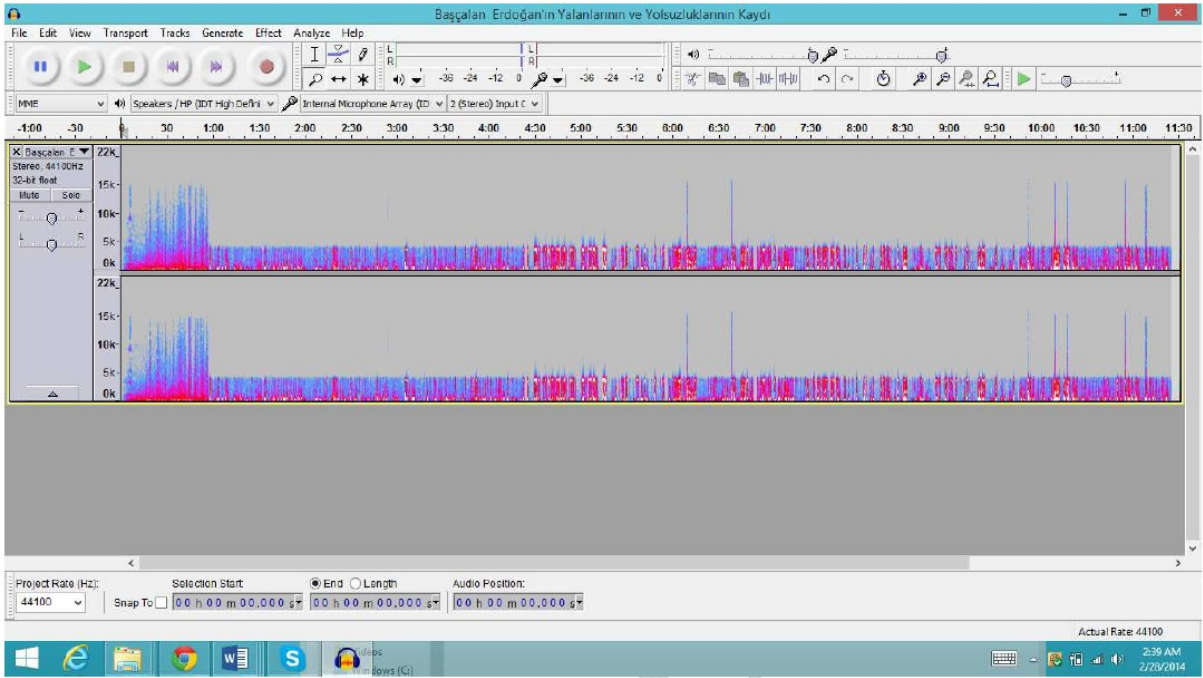
Türkçe arama kaydı, son birkaç dakikadaki “şaka” hariç, kesme, yapıştırma, kolajlama, veya herhangi bir tahrifatın olmadığı, birden fazla aramadan (boşluklar) oluşan bir kayıttır. Her ne kadar, orijinal kaydın dosyasına ulaşmadan ve kesintisiz bir delil zinciri olmadan, tamamiyle tahrifat yapılmamış bir kayıt olduğunu kanıtlamak mümkün olmasa da, bu noktada, kayıta herhangi bir şekilde tahrifat yapıldığını kanıtlamak mümkün değildir.

Ek 1: orijinal kayıtların başka bir kaynaktan kopyası

<https://www.youtube.com/watch?v=Cvf4aeRLu0E> - Başçalan Erdoğan'ın Yalanlarının ve Yolsuzluklarının Kaydı

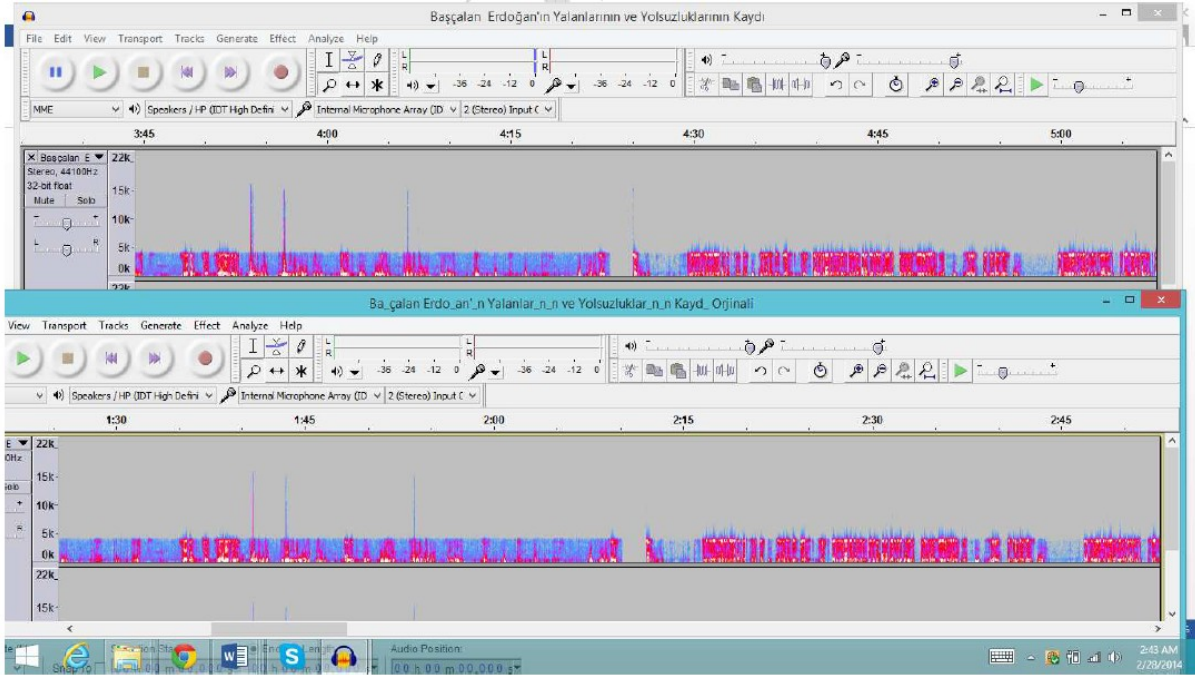
Yukarıdaki youtube linkini, ve youtube kaydını MP3'e çeviren bir çevrimiçi servisi kullanarak bu youtube videosunun MP3 hali elde edildi. McClatchy muhabiri Roy Gutman tarafından sağlanan kayda pek çok yönden benzerlik göstermekle birlikte, bazı farklılıklar da var. Bu sesin başlangıcında müzik var, ve bu zaman kodlarını saptırıyor. Son birkaç dakikada “şaka” kısmı yok.

Ancak, boşluklar, ve sıçramalar mevcut.



Karşılaştırmak adına, Roy Gutman'ın sağladığı kayıta 2:10'da bulunan boşluk, bu kayıta yaklaşık olarak 4.23'te yer alıyor.

Boşluklar, ve öncesindeki çeşitli ani yükselmeler, oldukça uyumlu olarak sıralanıyor.



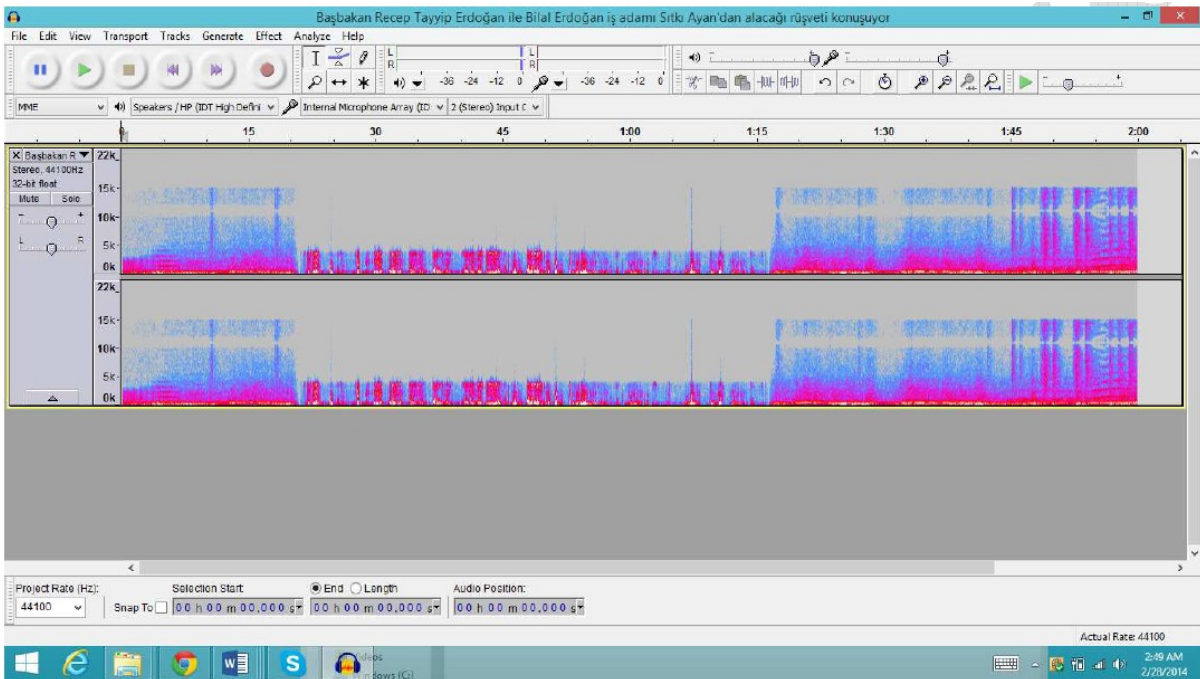
Kayıtlar, birinin başındaki müzik, ve diğerinin sonundaki “şaka” hariç, birbirine uyuyor.

Aynı sonuçlara varılabilir. Bu noktada, bunların yanlışlığı kanıtlanamaz.

Ek 2: İkinci kayıt grubu

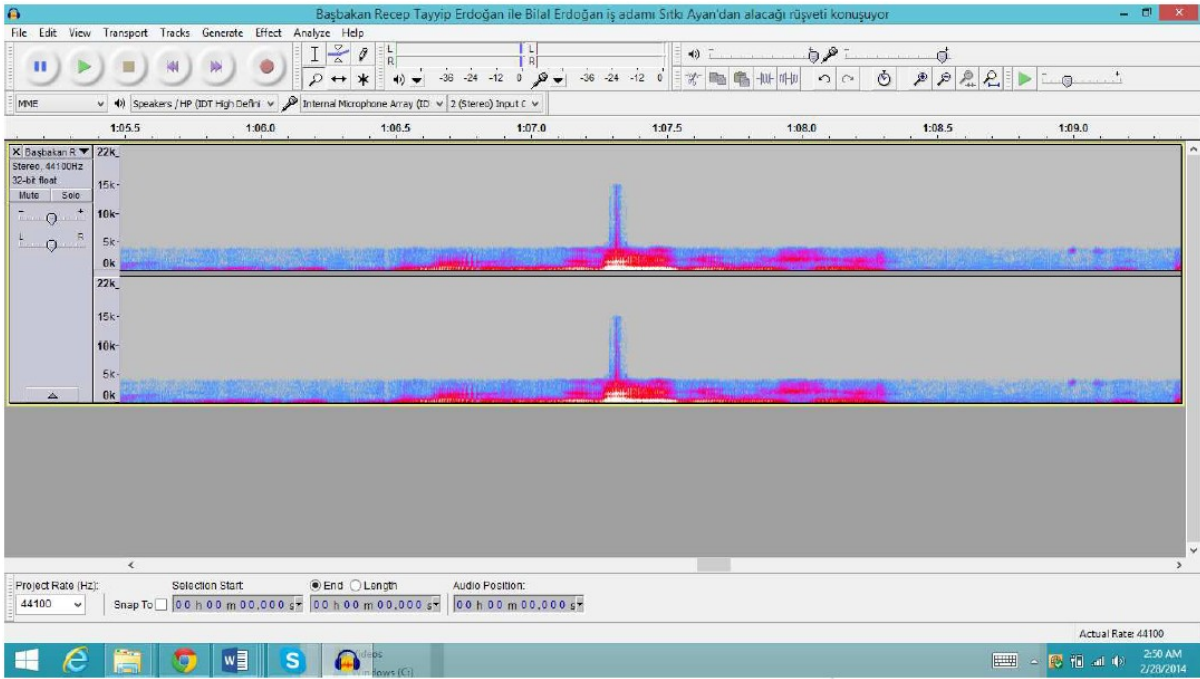
Bu Youtube linki kullanılarak, ikinci bir kayıt grubu elde edildi. Youtube kaydını MP3'e çeviren aynı çevrimiçi servisi kullanarak MP3 ses dosyası elde edildi ve önceki araçlar kullanılarak incelendi, bunlar, Windows 8.1 kurulu olan bir HP taşınabilir bilgisayar, ve Audacity programı.

<http://www.youtube.com/watch?v=Ya1iQvpXe60> – 2. set - Başbakan Recep Tayyip Erdoğan ile Bilal Erdoğan iş adamı Sıtkı Ayan'dan alacağı rüşveti konuşuyor



Kaydın başında ve sonunda yükseltilmiş olan gürültü tabanına dikkat edin. Bu müziktir ve hiçbir şekilde telefon kaydının kendisi ile ilgili değildir.

Aramadaki en büyük ani yükseliş, kaynağını ortaya çıkarmak için büyütüldü.



Oluşumu ve “görünüşü” ilk kayıt grubundaki ani yükselişlere benziyor. Ve yine, anlaşılan, kelimelerin seslendirilmesi başladıktan sonra, kesme ve yapıştırma veya seslerin montajlanması ihtimalden oldukça uzak.

Tekrar, bu noktada, bu kayıtlarla, orijinal ses dosyasına ulaşmadan ve kesintisiz bir delil zinciri olmadan, bunun yanlışlığı elimizdeki teknik kesinliğin sınırları dahilinde kanıtlanamaz.

Ek 3:

Şifreli telefonlar ve bu kaydın en başta nasıl elde edilmiş olabileceğine dair ilgi daha önce ifade edilmişti. Ancak lütfen not edin, bu tamamıyla varsayımlar ve tahminlere dayanıyor.

Şifreli telefonlar, genel olarak, şifrelenmiş bir bağlantı ile sunucuya ulaşır. Sunucu ve telefon belirli bir çift şifreye sahiptir. Bir şifre ile şifrelenmiş olan şey, diğer şifre ile açılır; bunun tam tersi de geçerlidir. Ancak, her telefonun ve sunucunun şifre çifti özgündür, sadece o telefon için geçerlidir. Bu pratikte şu anlama gelir, Telefon 1 sunucuya bağlanır. Telefon 2 sunucuya bağlanır. Telefon 1'i kullanan kişi sunucuya şifreli bağlantı ile ulaşır, sunucunun aktarması ile, şifreli bağlantı Telefon 2'ye ulaşır ve Telefon 2'yi kullanan kişi bunu duyar.

Sunucu Telefon 1 ve Telefon 2 giden tüm trafiği şifreleyen ve açan tüm anahtarlara sahip olduğu için, sunucuyu kontrol eden konuşmanın iki tarafını da dinleyebilir.

Bugün bilindiği kadarıyla, sadece tek bir şirket bunu engelleyebilecek kapasiteye sahip. Silent Circle, PGP (Pretty Good Privacy) şifrelenmiş eposta sistemini de yaratan kişilerin kurduğu, telefondan telefona şifreleme sistemini kullanır; telefondan sunucuya değil. Bu, “Zero-Knowledge” (Sıfır-Bilgi) sistemi olarak bilinir, ve burada sistemi çalıştıran kişiler dahi şifreleri açamaz ve sistemin kullanımı veya sistemdeki data konusunda bir bilgiye sahip değildir.

Kayıtlar:

Kayıtlardaki bir ortak nokta bu bağlamda çok dikkat çekici. Konuşmadaki genç adam daha yüksek sesli, daha net, neredeyse telefondaki mikrofonu zorluyor. Daha yaşlı olan adamın sesi daha kısık, belirsiz, hatta “çatlak/çatallı”.

Bunların sebebi bilinmiyor olsa da, birkaçı varsayılabilir.

1. Telefonlardan sadece biri şifreli olabilir, o telefon sesi sıkıştırıp, dijitalleştiriyor ve şifreliyor olabilir. Bu durumda, belirsizlik ve düşük ses volümü açıklanabilir.
2. Diğer taraftan, eğer genç adamın telefonuna böcek yerleştirilmişse, onun sesinin yüksekliği cihaza yakınlığı ile açıklanabilir. O böceğe doğrudan konuşuyordur, daha yaşlı olan adam ise telefonun iç hatlarıyla kayda alınıyordur, bu belirsizlik ve düşük sese neden oluyordur. Bu “böcek”, fiziksel bir dinleme cihazı olmak zorunda değil. Kötü niyetli bir yazılım da olabilir.
3. Bir son durumda, eğer her iki konuşan da şifreli telefonlarda iseler, ve hattı dinleme işlemi sunucudan yapılıyorsa, belki konuşan taraflardan biri basitçe kapsama alanının sınırında olabilir, bu da daha düşük iletim hızına neden oluyordur.

Kayıtlara dair sayılan tüm bu durumlar düşünce deneyleridir. Hiçbiri doğrudan gerçekler üzerine kurulmamıştır, çünkü gerçekteki şartlara dair hiçbir kesin bilgi sunulmamıştır. Bunlar ihtimaller olarak buraya dizilmiştir.

Bu rapor, bana ulaşan bilgiler dahilinde, ve benim sahip olduğum deneyim ve bilgi ölçüsünde doğrudur.

Joshua Marpet

Yönetici Müdür

Guarded Risk

28 Şubat 2014



Forensic Report – Preliminary

Joshua Marpet
Managing Principal

2/28/2014

Background:

This report is written by Joshua Marpet, Managing Principal of Guarded Risk. Joshua Marpet is an Adjunct Professor teaching Digital Forensics, Information Security, Ethics, and Ethical Hacking at Wilmington University, in the College of Technology, Computer Network Security program. Joshua is an Accessdata Certified Examiner (ACE) in the field of digital forensics. Joshua Marpet is a former Senior Information Security Analyst at the Federal Reserve Bank of Philadelphia. He is a co-organizer of the Security BSides Delaware series of Information Security Conferences, and is the Vice President of the Cloud Security Alliance, Delaware Valley Chapter (CSA-DV). His background includes being a police officer with the St. Tammany Parish Sheriff's Office before, during, and after Hurricane Katrina. Joshua Marpet's experience also includes work on video and audio surveillance systems around the world, including the Lower Manhattan Surveillance Initiative, Algerian military base fence alarm systems, and Newark Airport's tarmac surveillance, along with multiple prisons and casinos.

Request:

An MP3 file was provided, and a request was placed to determine, as conclusively as possible, if any "tampering" had been performed on the audio.

Issues:

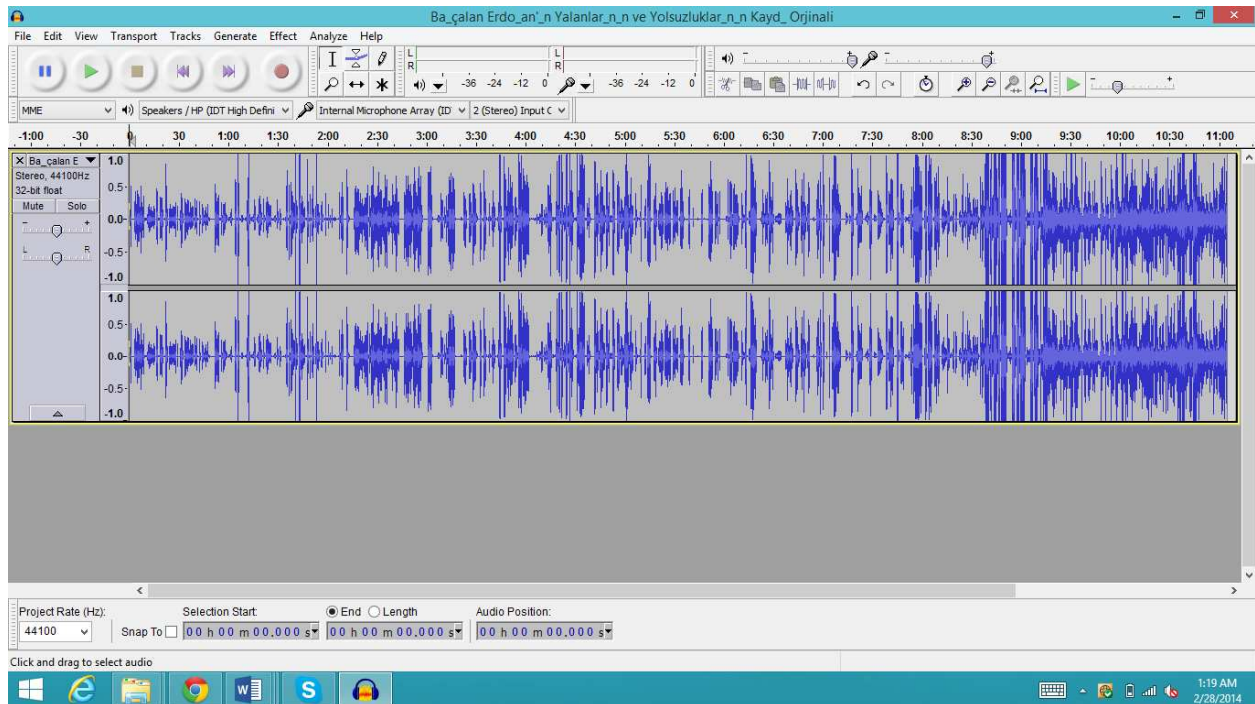
Not being a native Turkish speaker, it's difficult to determine intonation changes, nuances, tonal changes, and whether a word or phrase has ended abruptly, or out of sync. That being said, it was determined to perform a technical analysis of the audio, and confirm any anomalies or questions with the help of native Turkish speakers as part of the analysis.

Tools:

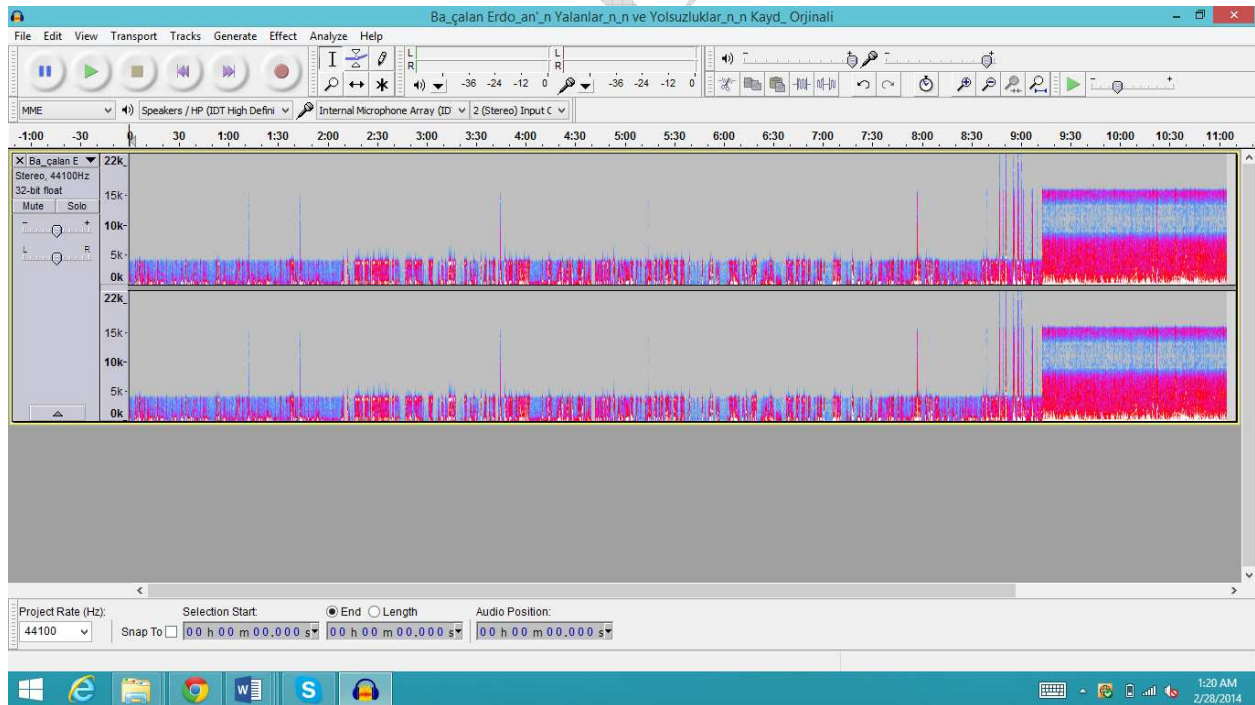
An HP laptop, running Microsoft Windows 8.1, and fully patched, was utilized to perform the analysis. The software used was Audacity from <http://audacity.sourceforge.net/>. It is a highly capable audio creation and editing software, used in multiple ways, from podcast creator and editor, to music editing and mixing. As an open source project, its code is examined and tested by hundreds of thousands of people.

Analysis:

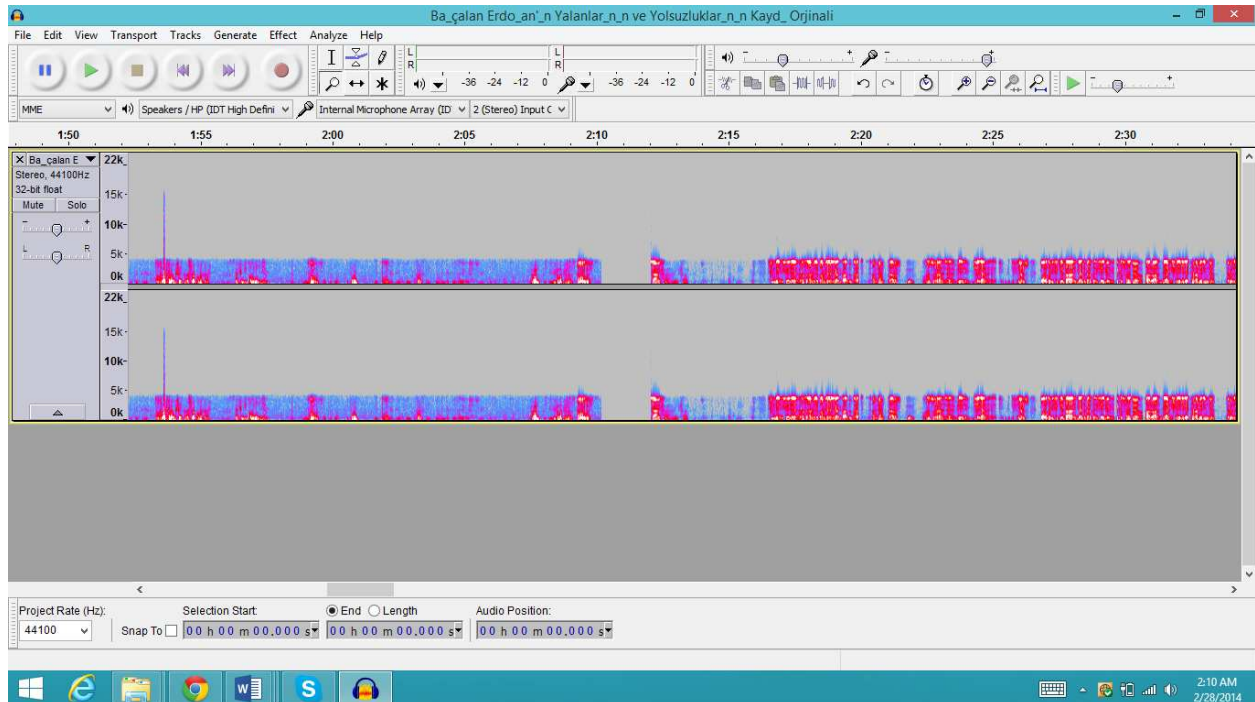
An MP3 file, named “Ba_çalan Erdo_an'_n Yalanlar_n_n ve Yolsuzluklar_n_n Kayd_ Orjinali.mp3”, was provided for analysis. Opening it in Audacity shows the waveform view, roughly correlating to volume.



Switching to Spectrogram view shows a frequency plot.



In this view, which was the primary view used for analysis, three sets of anomalies were discovered. It can be seen that while most of the conversation is on the same level, the “noise floor”, there are several frequency “spikes” scattered throughout the audio, and the last few minutes, from approximately 9:15 on, are on a totally different noise floor. The last set of anomalies can only be easily seen when zoomed in.



Between 2:10 and approximately 2:12, seen above, there is a gap with absolutely no sound at all. If this mp3 is played, even when there are no voices, there is environmental and electronic noise, from air conditioning, heating systems, line noise on the phone, etc. But from 2:10 to 2:12, there’s nothing at all.

One of the frequency “spikes” can be noted just before 1:54 in the figure above, as well.

Assuming malicious intent for all three sets of anomalies, the gaps could be indicative of cutting and pasting segments of sound, and the spikes attempting to change the tone, intonation, nuance, or meaning of a word or phrase. The raised noise floor and different voices for the last few minutes of audio could be indicative of a different type of bug, that of a room bug, rather than a phone bug. Alternatively, it could simply have been the same phone turned on it’s speakerphone.

Consultation with a Turkish speaker:

A Turkish speaker was consulted about the anomalies.

The first anomalous piece discussed was the gaps, such as the one at 2:10. As it turns out, the gaps are simply where the multiple recordings were placed together in one mp3 file. Not malicious at all.

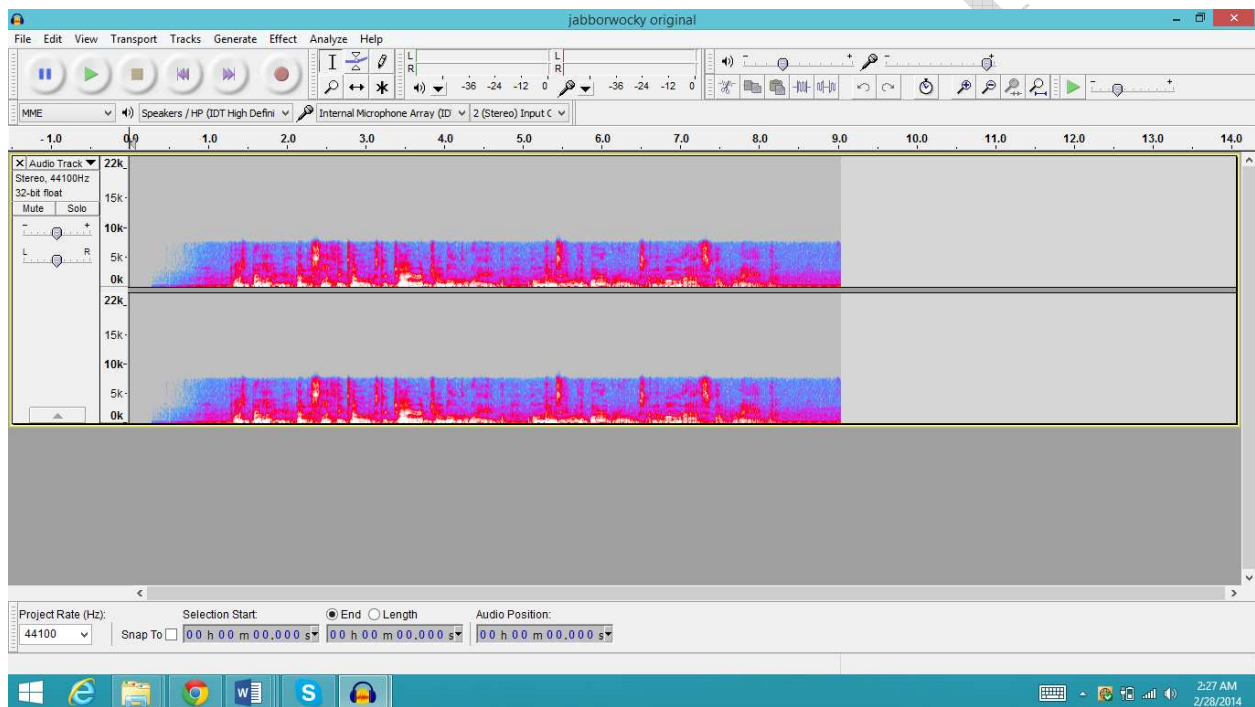
The raised noise floor of the last few minutes was identified as a joke, or added bit of dialogue with people not involved in the phone calls. It was speculated that they could be the people who leaked the phone calls?

The only anomaly that is unsolved is the “spikes”. The two possibilities discussed at that point were cutting and pasting of audio, or an attempt to change the tone, intonation, nuance, or meaning of a word or phrase. The Turkish speaker indicated that the tone, intonation, nuance, and meaning appeared to be natural, without artificial change. Also, the spikes occurred, almost without fail, after sound had already started, meaning that if they were an indication of cutting and pasting, the sound should have changed abruptly at those moments, in the middle of a word, for example.

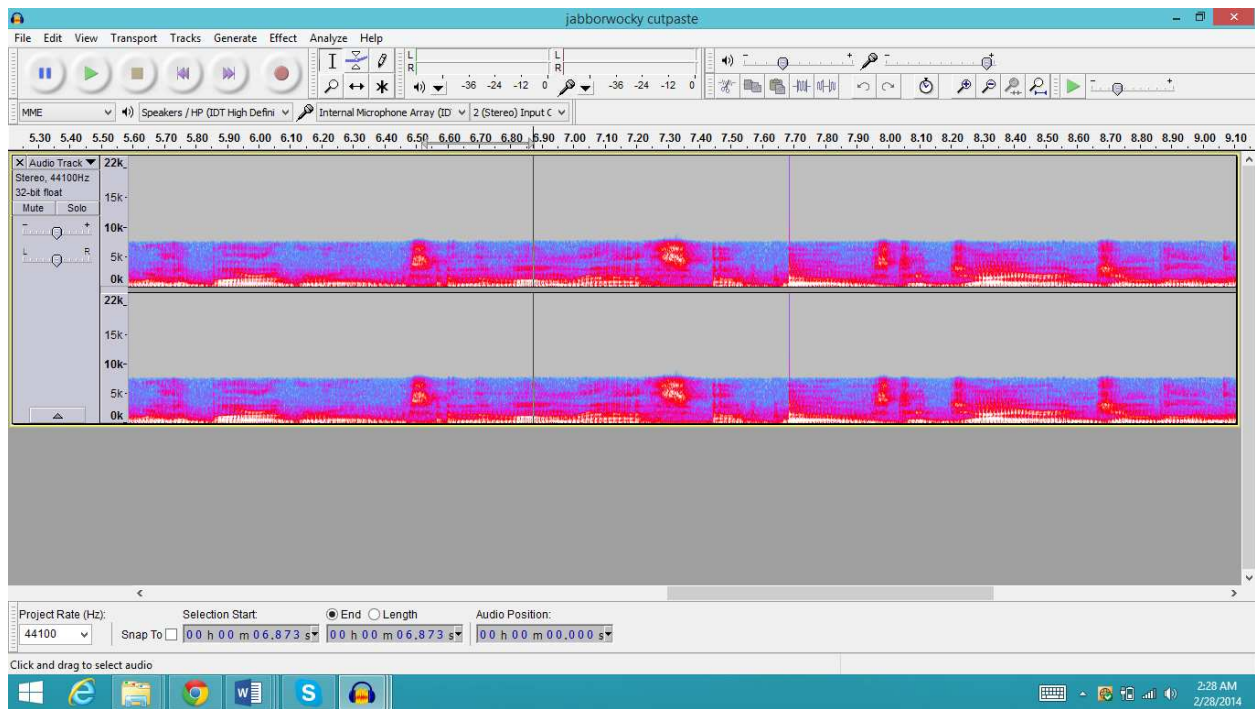
A supposition, or guess, is that the spikes are some sort of bookmark, or index. Many of them seem to be markings near or on names. This has not been explored due to time constraints.

Conclusions:

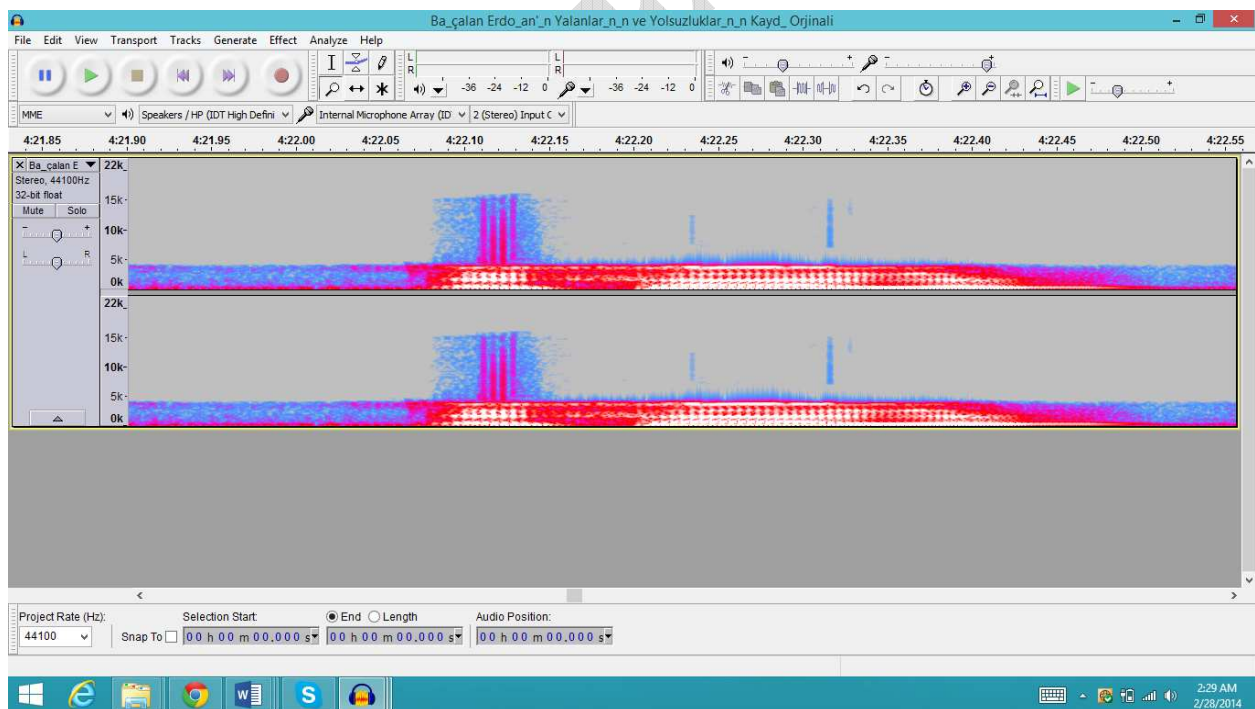
To check these conclusions and suppositions, a short audio track was recorded, using the HP laptop, and Audacity, listed above in the Tools section. Joshua Marpet recited the first verse of Lewis Carroll’s “Jabberwocky” poem. (Jabberwocky original).

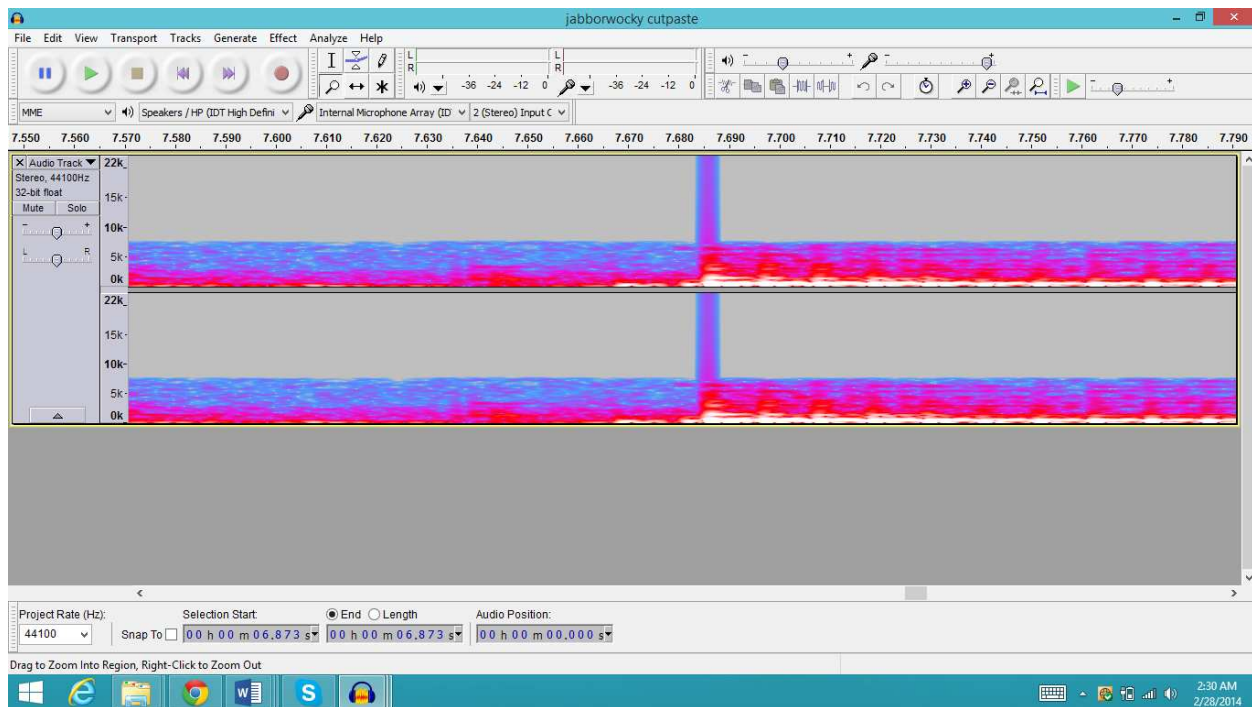


He then cut and pasted a short section of it, to a later area of the poem.



Notice the two spikes, which in some ways are similar to the frequency spikes in the first examined recording. However, they are different in some important ways. Upon zooming in, these ways become obvious.





Notice how clean the line is in the Jabberwocky recording, and how it reaches to the top of the channel/spectrogram. Notice how in the Turkish call recording, it is actually multiple lines, not clean at all, with much “static” around it, and how it does not reach to the top of the channel/spectrogram.

This indicates that the frequency spikes are indeed artifacts, but most likely from some line noise, clicking, or indeed, still possibly a bookmarking or annotation system. It was checked with the Turkish speaker, and most of the spikes in the Turkish call recording were in the middle of names and words. Any cut and paste would have mangled those names and words.

Final Conclusions:

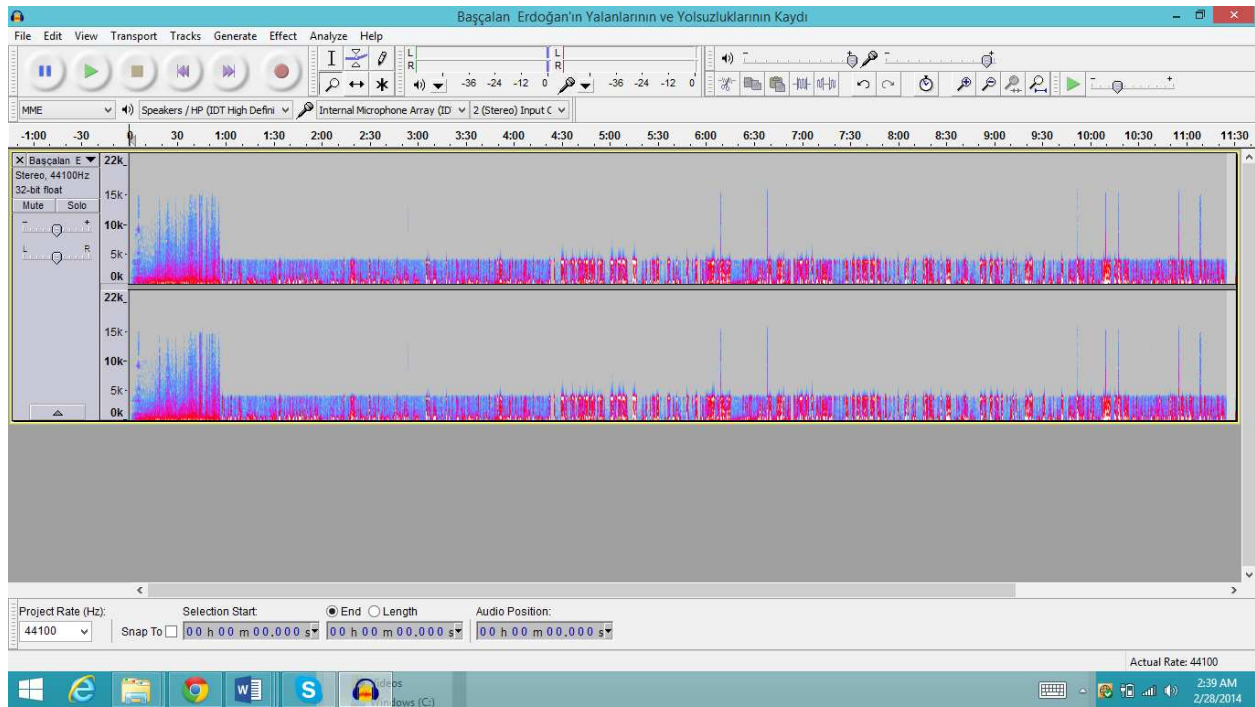
The Turkish call audio recording, minus the “joke” last few minutes, appear to be recordings of multiple calls (the gaps), without any cutting, pasting, collaging, or any tampering whatsoever. While it cannot be proven to be truly tamper free without access to the original source material, and an unbroken chain of custody, at this point, we are unable to prove that it was tampered with in any way.

Addendum 1: different source material for original set of recordings

<https://www.youtube.com/watch?v=Cvf4aeRLu0E> - Başçalan Erdoğan'ın Yalanlarının ve Yolsuzluklarının Kaydı

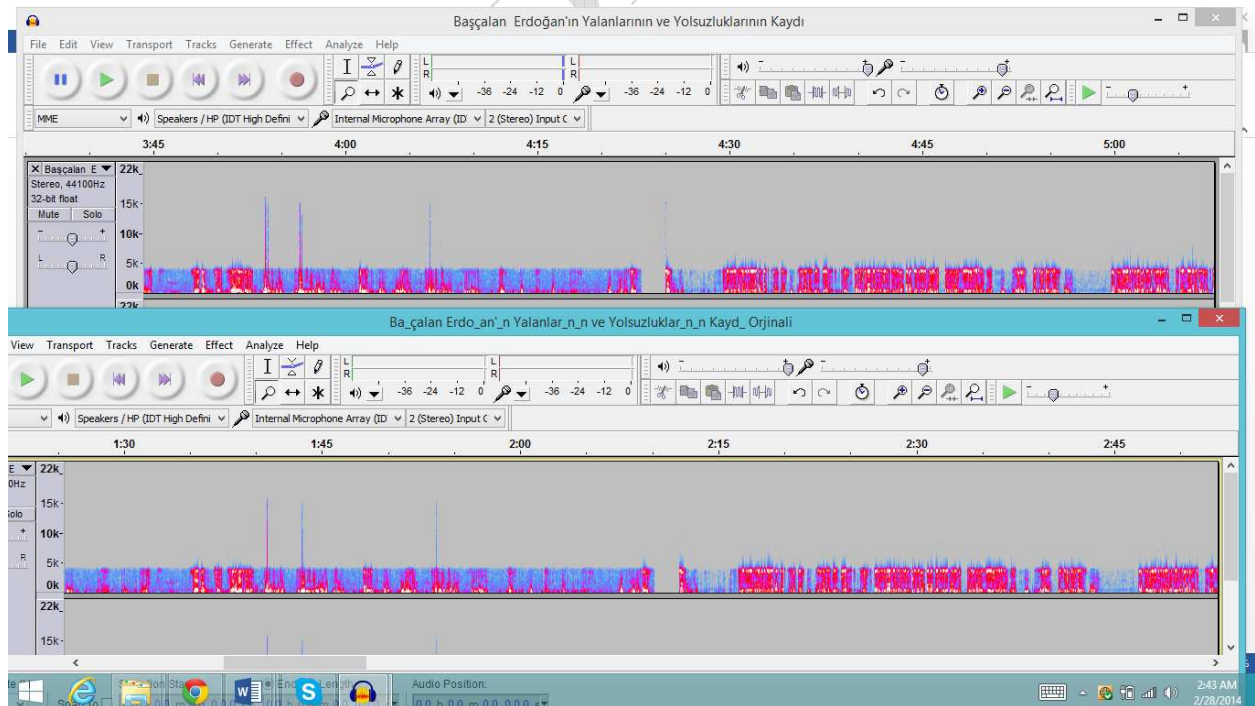
Using the above youtube link, and an online youtube to MP3 converter, an MP3 of this youtube video was obtained. While similar in many ways to the source material supplied by Roy Gutman, the McClatchy reporter, there are some differences. There is music at the start of the audio, skewing the time codes. The last few minutes do not have the “joke” section.

However, the gaps, and the spikes remain.



In order to compare, the gap that is found at 2:10 in the audio supplied by Roy Gutman, was located in this audio at approximately 4:23.

The gaps, and the several spikes preceding it, line up fairly precisely.



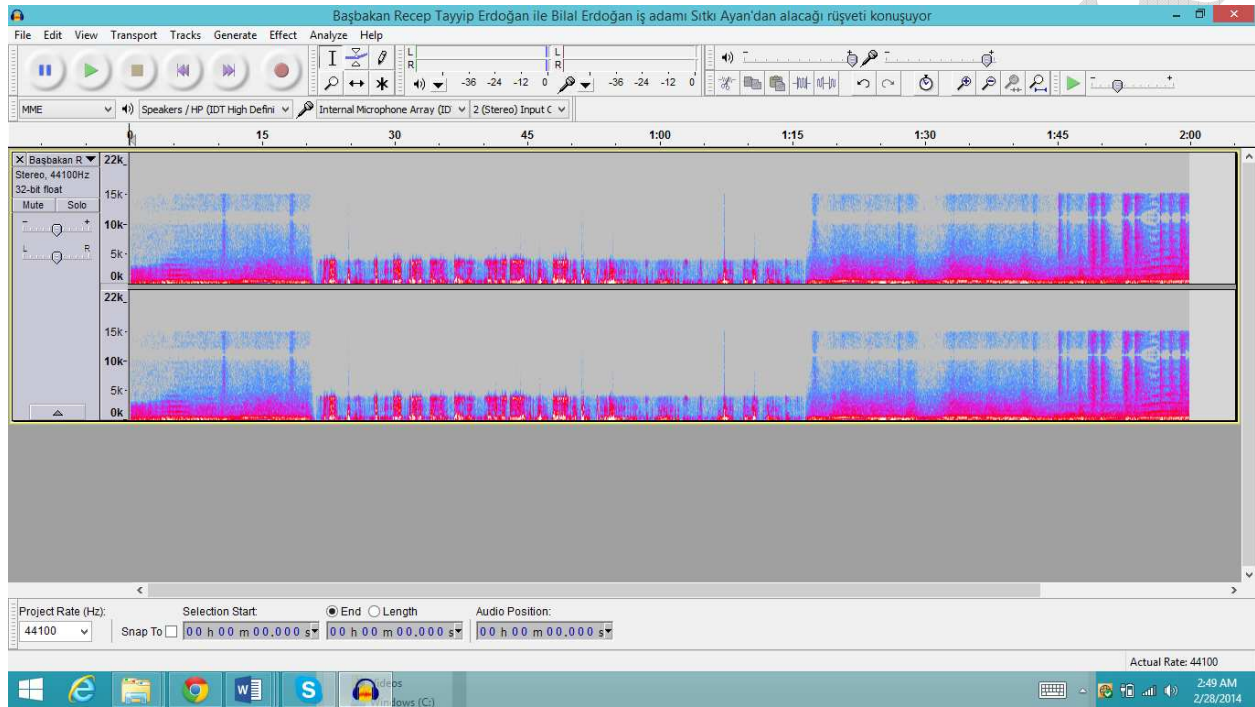
The recordings, minus the music at the start of the one, and the “joke” at the end of the other, matched.

The same conclusions can be drawn. At this time, they cannot be proven false.

Addendum 2: Second Set of recordings

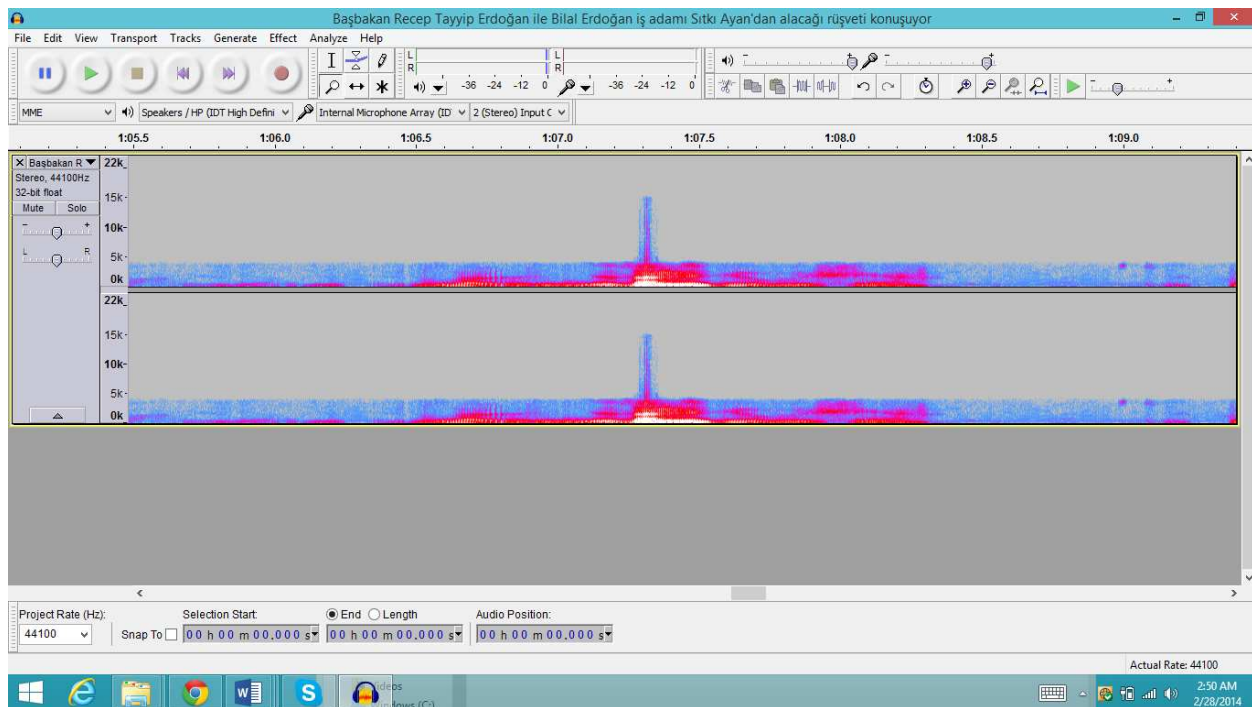
Using this Youtube link, a second set of recordings was obtained. Using the same online Youtube to MP3 converter, an audio file was obtained and examined using the same tools as before, namely, the HP laptop running Windows 8.1, and the Audacity software.

<http://www.youtube.com/watch?v=Ya1iQvpXe60> – 2nd set - Başbakan Recep Tayyip Erdoğan ile Bilal Erdoğan iş adamı Sıtkı Ay



Notice the raised Noise Floors at the beginning and end of the recording. This is music, and in no way relates to the phone call itself.

The largest spike in the call was magnified to determine its origin.



It is similar in composition, and in “look”, to the spikes from the first set of recordings. As it occurs, again, after vocalization of the word has started, it is extremely unlikely that it is a cut and paste, or montage of sounds.

Again, at this point, with this recording, and no access to original source material with an unblemished chain of custody, this cannot be proven to be false, to the limits of our engineering certainty.

Addendum 3:

Interest has been expressed in Cryptophones, and how the recordings might have been obtained in the first place. Please note, this is all supposition and informed guess.

Cryptophones, classically, have an encrypted tunnel with a server. The server and phone have a pair of keys. What is encrypted with one key can be decrypted with the other, and vice versa. But each phone and server key pair is unique, for that phone only. What that means, practically, is that Phone 1 connects to the server. Phone 2 connects to the server. Then the person holding Phone 1 can talk through the phone, down the encrypted tunnel, to the server, across the server, to the encrypted tunnel to Phone 2, where the person holding Phone 2 will hear it.

Since the server has the keys to decrypt and encrypt all traffic to and from Phone 1 and Phone 2, whoever controls the server can listen to both sides of the conversation.

As far as is known today, only one commercial company has the capability to avoid this. Silent Circle, which was formed from the same people who created PGP (Pretty Good Privacy) encrypted email, uses keys from phone to phone, not phone to server to phone. This is known as a “Zero-Knowledge” system, where even the people who run the system cannot decrypt or have any knowledge of the use or data on the system.

Recordings:

The recordings have one thing in common that is interesting in this context. The younger man on the calls is loud, clear, almost overpowering the microphone on the phone. The older gentleman's voice is quieter, and a bit fuzzier, or "pixilated".

While the reasons for this are not known, some can be supposed.

1. It is possible that one person was on a cryptophone, which compresses, digitizes, and encrypts the audio. In that case, the fuzziness and low volume could be explained by that.
2. On the other hand, if the younger gentleman's phone was bugged, then the loudness of his voice could be explained by the physical nearness of it. He would be speaking directly into the bug, while the older gentleman would be received through the phone circuitry, adding fuzziness and lowering the volume. Realize that the "bug" could be a software program, a piece of malware, rather than a physical bug.
3. One last case, if both parties were on cryptophones, and the intercept was from the central server, perhaps one of the parties was simply almost out of data range, resulting in lowered bandwidth.

All of these cases in this Recording segment, are thought experiments. None of them are based directly on reality, as no reliable information as to the real situations has been received. They are listed here as possibilities.

This report is the truth, with the information I have, and to the limits of the knowledge and experience I possess.



Joshua Marpet

Managing Principal

Guarded Risk

2/28/2014